

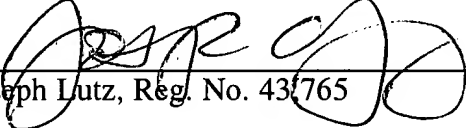
REMARKS

No new matter has been added to the specification and the claims. The specification and Claims 15-25 have been revised to more accurately define the invention disclosed in the patent application as filed on July 5, 2001.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: July 23, 2001



Joseph Lutz, Reg. No. 43,765

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

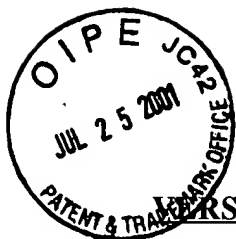
CERTIFICATE OF MAILING:

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: U.S. Patent and Trademark Office, Washington, DC 20231 on July 23, 2001.



Marilyn Bass

July 23, 2001



VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION

Paragraph [002] has been amended as follows:

[002] The advent of the Internet provides Internet users with a worldwide web of information at the click of a button. Accordingly, various businesses have responded to the incredible reach provided by the Internet to enable commerce via channels provided by the Internet. As such, the Internet has become a key mechanism for business to ~~commerce~~ consumer (B2C) and business to business (B2B) commerce. Moreover, many entertainment providers have been quick to utilize the Internet as an additional venue for presenting their entertainment content to users.

Paragraph [0036] has been amended as follows:

[0036] Referring now to FIG. 3, FIG. 3 depicts a block diagram illustrating a subset of the components of a conventional router 202. The router 202 includes a forwarding ~~plane~~ plane 280 containing an egress filter 206 and a forwarding decision block 290. The egress filter 206 drops traffic matching certain specifications as provided by the control plane 210. The forwarding decision block 290 decides how to forward the traffic. Accordingly, when a piece of network traffic (packet) is locally addressed, the forwarding decision block 280 forwards the packet to the control plane 210 where it is processed.

Paragraph [0037] has been amended as follows:

[0037] Otherwise, the forwarding decision block 280 determines (for example, using a look-up table) an egress port (or output port) and a next hop router through which to route the packet and then passes the packet to the egress filter ~~204~~ 206. Once determined, the forwarding plane sends the packet to one or more output/egress ports 210 (210-1, . . . , 210-N). Unfortunately, conventional routers require manual intervention to instruct the control plane to install a filter into egress filter ~~204~~ 206. For example, installation of filters into egress filter 200 is generally via the input of filters by an administrator at an administrator workstation.

IN THE CLAIMS

The claims have been amended as follows:

15. (Amended) A ~~computer-machine~~ readable storage medium including program ~~instruction-instructions~~ that ~~directed-direct~~ a ~~computer-system~~ to function in a specific manner when executed by a processor, the program instructions comprising:
receiving notification of a distributed denial of service attack;

establishing security authentication from an upstream router from which attack traffic, transmitted by one or more attack host computers, is received; and

once security authentication is established, transmitting one or more filters to the upstream router such that attack traffic is dropped by the upstream router, thereby terminating the distributed denial of service attack.

16. (Amended) The ~~computer-machine~~ readable storage medium of claim 15, wherein the instruction of detecting the attack traffic further comprises:
monitoring network traffic received by an Internet host; and
when a distributed denial of service attack is detected, notifying the Internet host of the distributed denial of service attack.

17. (Amended) The ~~computer-machine~~ readable storage medium of claim 15, wherein establishing security authentication further comprises:
transmitting a security authentication request to the upstream router including authentication information, the authorization information including a destination address of the attack traffic; and
receiving authorization for establishment of security authentication from the upstream router.

18. (Amended) The ~~apparatus-machine readable storage medium~~ of claim 15, wherein transmitting the one or more filters further comprises:
identifying attack traffic characteristics of the attack traffic received by an Internet host;
generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics;
digitally signing the one or more filters using a digital certificate of the Internet host; and
transmitting the one or more digitally signed filters to the upstream router.

19. (Amended) A ~~computer-machine~~ readable storage medium including program ~~instruction-instructions~~ that ~~directed-direct~~ a ~~computer-system~~ to function in a specific manner when executed by a processor, the program instructions comprising:
establishing a security authentication of a downstream device;
once security authentication is established, verifying that one or more filters from the downstream device select only network traffic directed to the downstream device; and
once verified, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the downstream device.

20. (Amended) The ~~apparatus~~ machine readable storage medium of claim 19, wherein establishing security authentication further comprises:

- receiving a routing protocol update from the downstream device;
- selecting authentication information from the received routing protocol update;
- authenticating an identity of the downstream device based on the selected authentication information;
- once authenticated, selecting the one or more filters from the received routing protocol; and
- authenticating integrity of the one or more filters based on a digital signature of the filters.

21. (Amended) The ~~apparatus~~ machine readable storage medium of claim 19, wherein verifying the one or more filters further comprises:

- authenticating a source of the one or more filters received as the downstream device;
- once authenticated, verifying that a router administrator has set a DDoS squelch time to live value for received filters;
- once verified, generating a filter expiration time for each filter based on the time to live, such that the filters are uninstalled once the expiration time expires;
- verifying that an action component of each of the filters is drop; and
- otherwise, disregarding the one or more filters received from the Internet host.

22. (Amended) The ~~apparatus~~ machine readable storage medium of claim 19, wherein verifying the one or more filters further comprises:

- selecting a destination address component for each of the one or more filters received from the downstream device;
- comparing the destination address components against an address of the downstream device;
- verifying that the selected destination addresses matches the downstream device address;
- and
- otherwise, disregarding the one or more filters received from the downstream device.

23. (Amended) The ~~computer~~ machine readable storage medium of claim 19, wherein establishing security authentication further comprises:

- receiving a request for security authentication including authentication information from the downstream device;
- selecting the authentication information from the security authentication request; and
- authenticating an identity of the downstream device based on the selected authentication information.

24. (Amended) The ~~apparatus~~ machine readable storage medium of claim 19, wherein installing the one or more filters further comprises:

selecting network traffic matching one or more of the filters received from the downstream device; and

dropping the selected network traffic such that attack traffic received from one or more attack host computers by the downstream device is eliminated in order to terminate a distributed denial of service attack.

25. (Amended) The ~~apparatus~~ machine readable storage medium of claim 19, further comprising:

determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received;

selecting a port from the one or more determined ports;

determining an upstream router coupled to the selected port based on a routing table;

securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and

repeating the selecting, determining, and forwarding for each of the one or more determined parts.